Appendix 1

Policy and Procedures
for undertaking Directed Covert Surveillance
and the use of Covert Human Intelligence Sources

Produced by:

- Internal Audit Services, April 2010
- Updated w.e. 1st November 2012
- Updated May 2014
- Updated June 2016
- UPDATED OCTOBER 2016
- UPDATED SEPT 2018

Formatted: List Paragraph, No bullets or numbering

Formatted: Indent: Left: 0 cm, Hanging: 0.95 cm, No bullets or numbering

CONTENTS

Formatted: Font: Not Bold

3. Procedure

APPENDIX 1

a) Flow Chart Directed Surveillance

b) Sample application form for use of Directed Covert Surveillance

APPENDIX 2

a) Flow Chart for the procedure for the Application to the Justice of the Peace for an order to approve the grant of a RIPA Authorisation or Notice

b) Copy application form and order for judicial approval

PART 1: POLICY FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. Introduction

1.1 The performance of certain investigatory functions of Local Authorities may require the surveillance of individuals or the use of informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. Legislation now governs how Local Authorities should administer and record surveillance and the use of informants and renders evidence obtained lawful for all purposes. This Policy sets out the Council's rules and procedures.

1.2 The purpose of this Policy is to ensure there is a consistent approach to the undertaking and authorisation of surveillance activity. Therefore, this Policy is to be used by all Council service areas and officers undertaking investigation work and using the techniques of surveillance or the use of Covert Human Intelligence Sources (CHIS's).

1.3 In this Policy the following terms shall have the meanings stated:

"**Investigating Officer**" – shall mean any Council Officer undertaking or wishing to undertake directed covert surveillance or to use a CHIS provided he / she has received appropriate training.

"**Authorising Officer**" – shall mean all Chief Officers and the following ~~Group Managers~~staff in the Department for ~~Place (Group Manager, Regulatory Services;~~ Group Manager, Waste & Environmental Care ~~and Group Manager, Partnership Community Safety)~~ and the Director of Public Protection who can authorise directed covert surveillance or the use of a CHIS provided he / she has received appropriate training. This role is currently held by two members of staff Steven Crowther and Carl Robinson.
stephencrowther@southend.gov.uk
carlrobinson@southend.gov.uk

"**Senior Responsible Officer**" – shall mean the ~~Head~~ Director of Legal & Democratic Services and a role currently held by John Williams.
johnwilliam@southend.gov.uk

"Principal Legal Executive" – shall mean the officer with this job title and a role currently held by Tessa O'Connell.
tessaoconnell@southend.gov.uk

Formatted: Left, Indent: First line: 0 cm
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Font color: Auto
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Left, Indent: Left: 0 cm, First line: 0 cm
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Font color: Auto
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Font color: Red
Formatted: Left
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Left, Indent: Left: 0 cm, First line: 1.27 cm
Field Code Changed
Formatted: Hyperlink
Formatted: Left
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Left, Indent: Left: 0 cm, First line: 1.25 cm
Field Code Changed
Formatted: Hyperlink
Formatted: Default Paragraph Font, Font color: Auto

1.4 ~~T~~This Policy was ~~further~~ updated in November 2012 to reflect the provisions of the Protection of Freedoms Act 2012 which from the 1st November 2012 requires that a Justice of the Peace ("JP") must approve all Local Authority RIPA applications and renewals.

Two guidance documents explaining this ~~new~~ authorisation process have been issued by the Home Office to Local Authorities and Magistrates and these are available on the following website:

~~I would put these docs on the intranet in a RIPA folder with the Codes etc as it stops you always having to check if the links are current.~~

This policy was again updated in June 2016 to incorporate additional information on surveillance outside RIPA in Section 6 and regarding the internet and social media in Section 8.

This Policy was also updated in September 2018 to reflect the changes in the August 2018 Codes of Practice.

~~I would remove all of the below I don't think it is needed. It then reads better.~~

~~Practice April 2010 to reflect the following Statutory Instruments and new codes of practice for Covert Surveillance and Covert Human Intelligence Source (CHIS):~~

- ~~The Regulation of Investigatory (Communications Data) Order 2010 [SI 2010/480].~~
- ~~The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 [SI 2010/521] together with an Explanatory Memorandum as amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 [SI 2012/1500].~~

- ~~The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2010 [2010/462] together with an Explanatory Memorandum.~~

- ~~The Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010 [SI 2010/463] together with an Explanatory Memorandum.~~

- ~~The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 [SI 2010/461] together with an Explanatory Memorandum.~~

Formatted: Font color: Accent 6
Formatted: Left, Indent: First line: 0 cm
Formatted: Font color: Accent 6
Formatted: Left, Indent: First line: 0 cm
Formatted: Font color: Accent 6
Formatted: Strikethrough

1.5 RIPA was overseen by the Office of Surveillance Commissioners (OSC). However, from 1 Sept 2017 oversight is now provided by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection regime whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA code applies, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.

1.6~~4~~ Failure to comply with RIPA ~~is likely to result in errors (see section ???) and may~~ may ~~may~~ leave the Council open to potential claims for damages or infringement of individual's human rights. It may also mean that any evidence obtained in breach of the provisions of RIPA is rendered inadmissible in Court.

~~1.5 This Policy was further updated in November 2012 to reflect the provisions of the Protection of Freedoms Act 2012 which from the 1st November 2012 requires that a Justice of the Peace ("JP") must approve all Local Authority RIPA applications and renewals.~~

~~Two guidance documents explaining this new authorisation process have been issued by the Home Office to Local Authorities and Magistrates and these are available on the following website:~~

~~**((((QUERY ?? are these the link needed?))))**~~

~~Is it?~~

~~https://osc.independent.gov.uk/wp-content/uploads/2016/07/OSC-Procedures-Guidance-July-2016.pdf~~

~~https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf~~

~~1.6 This policy was again updated in June 2016 to incorporate additional information on surveillance outside RIPA in Section 6 and regarding the internet and social media in Section 8.~~

1.6~~7~~ This is intended to be a best practice guide. It is not intended to replace the Home Office Codes and where necessary the Codes should be consulted.~~.~~ However, following the guide ensures compliance with the codes.

1.7 This is not intended to be an exhaustive guide and specific legal advice should be sought if officers do not find questions answered after reading

Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Indent: Left: 2.54 cm, No bullets or numbering
Formatted: Indent: Left: 0 cm, Hanging: 1.25 cm
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Left, Indent: Left: 0 cm, Hanging: 0.95 cm
Formatted: Default Paragraph Font, Font color: Auto
Formatted: Left, Indent: Left: 0 cm
Formatted: Font: Not Italic, Font color: Red
Formatted: Left, Indent: Left: 0 cm, Hanging: 0.95 cm
Formatted: Default Paragraph Font, Font color: Auto

this document and the Home Office Codes. Officers should always consult the Legal Team before seeking authorisation.

2. Background

2.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force making it potentially unlawful for a Local Authority to breach any article of the European Convention on Human Rights (ECHR). Any such breach may now be dealt with by the UK courts directly, rather than through the European Court at Strasbourg.

2.2 Article 8 of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of:

- National security
- Public safety
- The economic well-being of the country
- The prevention of disorder or crime
- The protection of health or morals
- The protection of the rights and freedoms of others

2.3 The performance of certain functions by Local Authorities may require the directed covert surveillance of individuals or the use of informants or undercover officers, known as CHIS.

Formatted: Font color: Red

2.4 Those who undertake directed covert surveillance on behalf of a Local Authority may breach an individual's human rights, unless such surveillance is consistent with Article 8 of the ECHR and is both necessary and proportionate to the matter being investigated.

2.5 As a result of the legislative changes referred to in 1 above, Local Authorities can now only authorise directed covert surveillance under RIPA for the purpose of preventing or detecting conduct which constitutes a **criminal offence** which is:

Formatted: Font: Bold

(a) punishable (whether on summary conviction or indictment) by a maximum term of at least six months imprisonment; or

(b) involves the sale of alcohol or tobacco to children.

2.6 Furthermore, if authorised by an authorised officer, –the Council's authorisation can only be given effect once an Order approving the authorisation has been granted by a JP.

Formatted: Font color: Red

2.7 Note

- A Local Authority cannot authorise the use of directed covert surveillance under RIPA to investigate low level offences e.g. littering, dog control and fly posting. Neither can a Local Authority authorise such surveillance for the purpose of preventing disorder, unless this involves a criminal offence punishable in the way described above.

- The crime threshold referred to above applies only to the authorisation of directed covert surveillance under RIPA, not to the authorisation of Local Authority use of CHIS or their acquisition of communications data.

2.8 In order to properly regulate the use of directed covert surveillance and the use of CHISs in compliance with the HRA, the Regulation of Investigatory Powers Act 2000 (RIPA) came into force on 25th September 2000.

2.9 RIPA requires that all applications to undertake directed covert surveillance of individuals or to use CHISs are properly authorised, recorded and monitored. This Policy sets out the procedures that need to be followed by officers of the Council prior to undertaking and during such activities, to meet the requirements of RIPA.

2.10 Failure to comply with RIPA may leave the Council open to potential claims for damages or infringement of individual's human rights. It may also mean that any evidence obtained in breach of the provisions of RIPA is rendered inadmissible in Court.

3. What is Surveillance?

3.1 Surveillance is:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.

- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

3.2 By its very nature, surveillance involves invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time. For example, within an individual's own home or private vehicle, an

individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

3.3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and require different degrees of authorisation and monitoring under RIPA.

3.4 **Overt surveillance** is where the subject of surveillance is aware that it is taking place. Overt surveillance is outside the scope of RIPA and therefore ~~does not contravene the HRA and therefore~~ does not require authorisation. ~~compliance with RIPA.~~ ~~Therefore~~ The codes also provide guidance that authorisation under RIPA is not required for the following types of activity: ~~surveillance of the following kinds:~~

- General observations that do not involve the systematic surveillance of an individual or a group of people.
- Use of overt CCTV surveillance.
- Surveillance where no private information is likely to be obtained
- Use of overt ANPR systems to monitor traffic flows or detect motoring offences.
- Surveillance undertaken as an immediate response to a situation.
- Review of staff usage of the internet & e-mail (but see Section 6 below).
- Surveillance not on statutory grounds. (see section 6 Surveillance outside of RIPA)

3.5 **Covert surveillance** is defined as "surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place" and is covered by RIPA. Covert surveillance is categorised as either intrusive or directed.

3.6 **Intrusive ~~covert~~ surveillance** is defined as covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. RIPA does not empower Local Authorities to authorise or undertake intrusive covert surveillance. Other means of investigation should be considered. ~~I need to check see if there is more on this anywhere~~

Formatted: Font color: Red
Formatted: Strikethrough
Formatted: Font color: Red
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Strikethrough
Formatted: List Paragraph, Left, No bullets or numbering
Formatted: Font color: Red
Formatted: List Paragraph, Left, No bullets or numbering
Formatted: Font color: Red
Formatted: Strikethrough
Formatted: Font color: Purple

3.7 **Directed covert surveillance** is surveillance which is covert but not intrusive and undertaken:

- For the purposes of a planned specific investigation or operation;
- In such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically targeted for the purposes of an investigation or operation);and
- Other than by immediate response to circumstances when it would not be practical to seek authorisation, for example, noticing suspicious behaviour and continuing to observe it.

3.7.1 **Private information** includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family11 and professional or business relationships. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

~~The above is updated from the codes~~

~~**Private information** should be interpreted to include any information relating to a personsn individuals private, family or working life. The concept of private information should be taken generally to include any aspect of a person's private or personal relations with others, including family and professional or business relationships. Family life should be treated as extending beyond the formal relationships created by marriage.~~

3.7.2 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

Formatted: Font: Bold, Font color: Red

Formatted: Font color: Red

Formatted: Font color: Accent 6

Formatted: Strikethrough

Formatted: Font: Bold, Strikethrough

Formatted: Strikethrough

Formatted: Font color: Red

~~Whilst a person may have a reduced expectation of privacy when in a public place; directed covert surveillance of that person's activities in public may still result in the obtaining private information.~~

Formatted: Strikethrough

Formatted: Strikethrough

3.7.3 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of directed covert surveillance of a person having a reasonable expectation of privacy authorisation is required.

3.7.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

Formatted: Font color: Red

3.7.~~5~~4 Directed covert surveillance involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. Private information may include personal data such as names, telephone numbers and address details.

3.7.~~6~~5 Directed covert surveillance does not include entry on or interference with property or wireless telegraphy but may include the use of photographic and video equipment (including the use of CCTV).

3.7.~~7~~6 Directed covert surveillance is covered by RIPA and requires prior authorisation.

4. What is a Covert Human Intelligence Source (CHIS)?

4.1 A CHIS is defined in section 25(7) of the RIPA as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

(a) Covertly uses such a relationship to obtain information or to provide access to any information to another person; or

b) Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

4.2 By virtue of section 26(9)(b) of RIPA a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

4.3 By virtue of section 26(9)(c) of RIPA a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

Vulnerable and Juvenile Sources

4.4 Special consideration must be given to the use of Vulnerable Individuals for CHIS. A 'Vulnerable Individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a Juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in his absence, the Deputy Chief Executive).

4.5 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.

4.6 Legal advice must be sought if considering using a vulnerable or juvenile CHIS.

4.~~7~~4 **It is not anticipated that CHISs will be ~~used~~ used often in the normal course of Council investigatory activity.** Any Council Officer considering the use of a CHIS must first contact the Senior Responsible Officer or the Principal Legal Executive to discuss the suitability of this approach.

4.~~8~~5 Authorisation is not required when individuals, including members of the public, are requested to provide information pertaining to other individuals, unless they are required to form a relationship, or manipulate an existing relationship with those other individuals.

5. Procedural principles for Surveillance and use of CHIS's

Formatted: Font: Bold, Font color: Red
Formatted: Font: Bold, Font color: Red
Formatted: Font: Bold
Formatted: Font: Bold, Font color: Red
Formatted: Indent: First line: 0.95 cm
Formatted: Indent: Left: 0 cm, Hanging: 0.95 cm
Formatted: Font color: Red
Formatted: Indent: Left: 0 cm, Hanging: 0.95 cm
Formatted: Font: Bold
Formatted: Font color: Red

5.1 Comprehensive procedures for undertaking directed covert surveillance and the use of CHISs are given in Parts 2 and 3 of this Policy respectively.

5.2 The conduct of surveillance which is consistent with these procedures can be undertaken with confidence that any evidence obtained will be admissible in a criminal trial, provided the conduct is authorised and is carried out in accordance with the authorisation. The authorisation must be shown to be necessary on the grounds of preventing or detecting crime (see 2.5 above).

5.3 The Investigating Officer seeking authorisation for directed covert surveillance or CHIS activity and the Authorising Officer must give consideration to the following factors:

- **Necessity** – on the statutory grounds (Criminal offence 6 months imprisonment or relate to the sale of alcohol or tobacco to children) and Is directed covert surveillance or CHIS activity the only or best way to obtain the desired information, or are other less invasive methods appropriate?

- **Proportionality** – Is the surveillance activity or CHIS activity proportional to the evidence that will be obtained and to the privacy the subject could reasonably expect? The methods used to obtain evidence should not be excessive and should be as non-invasive as it possible. The surveillance should not restrict an individual's right for privacy more than is absolutely necessary.

- **Collateral Intrusion** – Will the surveillance result in the observing of innocent people? If so can it be avoided or minimised?

5.4 Further Considerations:

- Does the application relate to a prevalent offence which has a maximum sentence of at least 6 months or relate to the sale of alcohol or -tobacco to children

- Have other ways of getting the information been investigated?

- Is surveillance a reasonable approach and "not a sledge hammer to crack a nut"?

- The risk of the direct surveillance and CHIS activity must be considered and managed.

- Surveillance authorisations remain valid for 3 months but must be cancelled prior to that if no longer required.

Formatted: Font color: Red

- CHIS authorisations remain valid for 12 months and must be cancelled prior to that if no longer required.

- Authorisations should be periodically reviewed by the Authorising Officer and the need for continued surveillance or CHIS activity ascertained; if no longer required authorisations should be cancelled.

5.5 All officers undertaking directed cover surveillance or wishing to use a CHIS must have received appropriate training to enable them to undertake this task.

5.6 Training should be periodically arranged to ensure that sufficient Authorising Officers are available.

5.7 Where directed cover surveillance or the use of a CHIS is likely to result in the obtaining of confidential information, it is imperative that legal advice should first be sought from the Senior Responsible Officer or the Principal Legal Executive. Confidential information includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.

5.8 The application for authorisation must include the following elements and the Authorising Officer must consider these, before authorising the directed covert surveillance or CHIS activity:

- full details of the reason for the directed covert surveillance or CHIS activity and the intended outcome;

- the proposed surveillance activity described as fully as possible, with the use of maps or other plans as appropriate;

- the necessity and proportionality to the potential offence consideration and whether other methods of less intrusive investigation should / have been attempted and whether they are appropriate;

- the resources to be applied and tactics and methods should also be included;

- the anticipated start date and duration of the activity, if necessary broken down over stages;

- details (including unique reference number) of any surveillance previously conducted on the individual.

5.9 In addition the Authorising Officer should notify the Chief Executive and Town Clerk of an authorisation.

5.10 Services that undertake surveillance activity or use of CHISs should put in place adequate arrangements for the retention of evidence gathered. The arrangements must comply with the Criminal Procedure and Investigations Act 1996 and any other relevant guidance or procedures to ensure the integrity of the evidence.~~.~~

5.11 Evidence or intelligence obtained as a result of a RIPA authorisation should not be passed to other agencies such as the Police unless the request meets the Data Protection Act 2018 requirements under the ~~.~~ Law Enforcement processing procedures or Schedule 2, Part 1 Paragraph 2 the replacement for ~~ThereforeTherefore, a~~ section 29 DPA ~~form should be received by the officer in charge of the Council investigation.~~ This will assist with oversight of the process.

5.12 The Authorising Officer's statement on the authorisation form should clearly demonstrate agreement that the activity is necessary and proportionate and that he / she has thoroughly considered the matter before authorising and state exactly what activity is authorised, against whom, where and in what circumstances.~~.~~

5.13 The responsibilities of the Senior Responsible Officer are:

- Maintaining the Council's RIPA Policy and Procedures
- Ensuring the integrity of the processes in place within the Council to authorise directed covert surveillance
- compliance with the legislation and Codes of Practice
- engagement with the Office of Surveillance Commissioners ("OSC") and inspectors when they conduct their inspections,
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner; and
- for ensuring that all *Authorising Officers* are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners. Where an inspection report highlights concerns about the standards of A*uthorising Officers*, this individual will be responsible for ensuring the concerns are addressed.

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Strikethrough

Formatted: Strikethrough

5.14 The Principal Legal Executive will maintain a Central Record of RIPA Applications and Authorisations (including the JP approval form). This Central Record will be used to track the progress of authorisations and ensure that reviews, renewals and cancellations take place within the prescribed timeframe. Copies of all RIPA authorisations, reviews, renewals and cancellations should be forwarded to the Principal Legal Executive promptly. The record will be available to the Office of Surveillance Commissioners ("OSC"), at any time. The Central Register format will be consistent with that detailed in the Home Office Code of Practice. ~~CHECK HOW GET UNIQUE NO~~

Formatted: Font color: Accent 6

5.15 A report on the use of RIPA will be submitted to the first Cabinet in the municipal year. Cabinet will consider this Policy and review the Council's use of RIPA.

5.16 The head of each section which undertakes directed surveillance or CHIS activity will ensure that:

- staff receive the necessary training;
- all activity is in accordance with RIPA, the Codes of Practice and this Policy; and
- relevant procedures are maintained to ensure the above.

6. Surveillance outside of RIPA

6.1 As a result of the change in the law from the 1st November 2012 directed surveillance under RIPA will only apply to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more or relates to the sale of alcohol or tobacco to children. This essentially excludes surveillance of many offences that the Council may investigate such as disorder (unless it has 6 months custodial sentence) and most summary offences such as littering, dog fouling etc. Other examples are referred to below.

6.2 This change does not mean that Council enforcement officers cannot undertake such surveillance, but because it is **not** regulated by the OSC, responsibility for monitoring this type of activity falls to the Council's Senior Responsible Officer (SRO). As a result procedures need to be in place to ensure that the Council can prove that it has given due consideration to necessity and proportionality which are central tenets of European Law and the likely grounds of any challenge.

6.3 If it is necessary for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation, such as in cases of

disciplinary investigations against staff or surveillance relating to Anti-Social Behavior appertaining to disorder. The Council must still meet its obligations under the Human Rights Act and be able to demonstrate that its actions which may infringe a person's article 8 rights to privacy are necessary and proportionate, which includes taking account of the intrusion issues. To demonstrate this accountability, the decision making process and the management of such surveillance must be documented. Therefore, should staff have a requirement to undertake such surveillance outside of RIPA, they should complete the Non RIPA Surveillance form (available from the RIPA pages on the intranet). This should be submitted to one of the RIPA Authorising Officers listed within this Policy to be considered for authorisation before any activity can be undertaken. There will be no requirement to have the authorisation approved by a Justice of the Peace. Should the activity be approved, the procedures to be followed will be the same as any RIPA authorised activity. Therefore, the Council expects that the procedure and management of the activity, from the initial surveillance assessment, through to completion and cancellation to be managed appropriately at the same level that the RIPA legislation and guidance requires. For further advice, refer to the RIPA pages on the Intranet.

6.4 Examples of Surveillance outside of RIPA

6.4.1 Planning

Some planning scenarios require evidence to be gathered either before service of a notice or post service of a notice to establish whether the notice has been breached. A common example may be some someone running a car repair business from home. It is often the case that this causes disruption and disturbance to neighbours who complain. Diary sheets may be issued to establish the level of activity and the person may be spoken to by a Planning Enforcement officer. It is often the case that the person states they only repair a few cars as a hobby for friends and family and are not running a business. At some stage it may be necessary for a Notice to be issued to the person. The repairs may then continue with the neighbours complaining. It is at this stage that targeted covert surveillance may be required as the best means of gathering the required information to establish if the Notice has been breached which would be a criminal offence. The offence does not meet the 6 months imprisonment criteria for it to be RIPA surveillance.

6.4.2 Social Services

Other examples may be Social Services investigations to protect vulnerable persons such as children. These would not be treated as criminal investigations and are normally dealt with in the Family Court. There may be occasions where some form of targeted covert surveillance activity is required to gather evidence for decision making or court proceedings. It is often the case that this type of surveillance is carried out by outside contractors. If this is the case the above procedure for surveillance outside of RIPA should be followed in order to demonstrate that the Council has considered the activity

with regard to Necessity and Proportionality and taken account of the intrusion on anyone.

6.4.3 Disciplinary Investigations
There may be serious disciplinary investigations that require some form of targeted covert surveillance activity which will engage article 8 rights to privacy. There is specific guidance issued by the Information Commissioners Office (ICO) in the Employment Practices Code under Part 3 Monitoring at Work. This guidance make it clear that surveillance should only be used for serious matters and that the activity must be Necessary and Proportionate taking account of the intrusion issues.

6.4.4 In the above scenarios, if these issues were criminal investigations and the offences carried the required sentence of 6 months imprisonment they would be meet the Directed Surveillance criteria under RIPA and would require authorisation. However these scenarios are to be treated as targeted surveillance operations outside of RIPA and the procedure for surveillance outside of RIPA should be followed in order to demonstrate that the Council has considered the activity with regard to Necessity and Proportionality and taken account of the intrusion on anyone.

6.5 Other routine activity that may be surveillance

6.5.1 There are other routine scenarios that may amount to surveillance under the definition contained within the Codes of Practice and this Policy such as the **deployment of a noise recording machine,** which may be monitoring persons and conversations etc. In these ~~instances~~instances, the persons responsible for the noise are notified that the recording activity may take place, which would give them a reduced expectancy of privacy. However, the Council still has an obligation to consider the intrusion issues and Necessity and Proportionality which will include the management and disposal of any personal data obtained. ~~Therefore~~Therefore, staff should carry out some form of privacy impact assessment and be able to demonstrate why it was necessary to deploy the noise machine and that it was a proportionate response to the problem to be resolved. It is likely that this can be documented and managed within the case notes of that particular complaint.

6.5.2 Internet and Social Media Investigations ~~(See further at Section 8 below)~~

Formatted: Strikethrough

Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

6.5.3 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breeches of privacy under Article 8 Human Rights Act (HRA) and other operational risks. The activity may also require a RIPA authorisations for Directed Surveillance

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm, No bullets or numbering

or CHIS. Where this is the case, the application process and the contents of this policy is to be followed.

6.5.4 Where the activity falls within the criterial of surveillance or CHIS outside of RIPA, again this will require authorising on a non RIPA form which will be authorised internally.

6.5.5 **There is a detailed separate corporate policy which deal with online open source research which should be read and followed in conjunction with this policy.**

~~Enquires by checking the internet and Social Media such as Facebook within investigations and complaints has now become common practice. However, it is well documented that these types of enquiries are no different to any other type of enquiry and may amount to Directed Surveillance under RIPA or Surveillance outside of RIPA. In either case the procedures in this Policy should be followed.~~

~~Whether the activity amounts to surveillance or not, staff have an obligation to consider Necessity and Proportionality and take account of the intrusion issues in all cases. The Council is a Public Authority in law and therefore has to take account of the HRA, which in turn means that staff have to take account of the legislation and be able to justify their actions. There is likely to be a considerable amount of intrusion with the likelihood of obtaining personal data when carrying out internet investigations or research. Privacy impact assessments should be carried out for internet research which should be ongoing. The OSC have advised carrying out a privacy assessment, which should be ongoing. The activities should be compliant with the HRA legislation, whether carried out within RIPA or outside of the RIPA legislation. The key issue is accountability and recording what and why the activities were taken.~~

~~The repeat covert viewing of someone's Social Media is likely to amount to monitoring which would be surveillance. Most activities will involve obtaining private information. If this is the case, and if the offences under investigation are criminal and have a sentence of 6 months imprisonment, an authorisation under RIPA should be considered. To covertly infiltrate a closed group in connection with a criminal investigation is likely to amount to a CHIS.~~

~~Most enquiries carried out by staff are not RIPA type enquiries. They may be to research a complaint or enquiry, which is not a RIPA scenario. Common internet checks are carried out to research a person's story to check it against their claim for something from the Council such as a homelessness claim. Checks are also carried out re debt recovery. Planning or licensing staff may check to see if someone is adhering to their licence.~~ ~~ALL CAN NOW GO~~

7. Use of CCTV

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

Formatted: Font: Bold

Formatted: Indent: Left: 0 cm, Hanging: 0.95 cm, No bullets or numbering

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Font color: Red, Strikethrough

Formatted: Strikethrough

Formatted: Font color: Accent 6, Not Strikethrough

Formatted: Strikethrough

Formatted: Left, Indent: Left: 0 cm, Hanging: 1.27 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

7.1 The use of the CCTV systems operated by the Council do not normally fall under the RIPA regulations. However, it does fall under the Data Protection Act 2018 ~~1998~~ and the Council's CCTV Policy. Guidance on their operation is provided in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner. Public authorities should also be aware of the relevant Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information"). ~~However, s~~Should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under directed covert surveillance and therefore require an authorisation.

7.2 On the occasions when the CCTV cameras are to be used for directed covert surveillance, either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, either the CCTV staff are to have a copy of the ~~notes~~ of the application form in a redacted format, or at least a copy of the authorisation page. It is important that the staff check the authority and only carry out what is authorised.

7.3 Operators of the Council's CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged, systematic surveillance of an individual may require an authorisation.

~~**8 Using the Internet to Conduct Online Covert Activity**~~

~~8.1 The internet is a useful investigative tool, giving access to a large amount of information which could not otherwise be obtained. The techniques and websites used change frequently and so it is difficult for definitive guidance to be written by the IPCO, the OSC as, by the time it is published, it may be obsolete. There is also a lack of definitive case law in this area. However, there is no doubt that these types of enquiries pose a risk to the Council for breaches of privacy and non-compliance with RIPA.~~

~~8.2 The Codes of Practice at 3.10 2.29 now provide guidance regarding the use of the internet to conduct covert enquiries. Therefore, the guidance provided in the codes of practice have been replicated in full to avoid confusion.~~

~~8.3 Code 2.29 states "The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights,~~

Formatted: Font color: Red
Formatted: Strikethrough
Formatted: Font color: Red
Formatted: Strikethrough
Formatted: Font color: Red
Formatted: Strikethrough
Formatted: Font color: Red, Strikethrough
Formatted: Strikethrough
Formatted: Font color: Red, Strikethrough
Formatted: Strikethrough
Formatted: Font color: Accent 6
Formatted: Strikethrough

~~including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this Code. Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered".~~

~~8.4 There is no doubt that certain conduct of repeat viewing, partculary of Social Networking Sites may meet the test of surveillance. If this activity meets the test for Directed Surveillance then a RIPA authorisation should be sought.~~

~~8.5 If it does not meet the Directed Surveillance criteria it is essential that detailed notes be made by any officer viewing material on the internet explaining what they were seeking, why it was necessary and proportionate to do so and why prior authorisation was not sought. Where material is printed or saved consideration must be given to the management of collateral intrusion – there may be personal data of people not subject to the investigation and this must be managed appropriately.~~

8.6 ~~There is other guidance available issued by the OSC which can be provided should staff require additional information. This can be obtained by contacting Head of Legal and Democratic Services or the Principal Legal Executive~~

~~**Removed as its now in the codes**~~

8 Use of material as evidence

8.1 Material obtained through directed surveillance, or entry on, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 198470 and the Human Rights Act 1998.

8.2 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the Criminal Procedure and Investigations Act 1996 and these considerations will apply to any material acquired through covert surveillance or property interference that is used in evidence When information obtained under a covert surveillance authorisation is used evidentially, it will be necessary to be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

9 Safeguards of Material

9.1 The Council and all staff should ensure that their actions when handling information obtained by means of covert surveillance comply with the

Formatted: Strikethrough

Formatted: Font color: Accent 6

Formatted: Font: Bold

Formatted: Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: Bold

Dtata Protection Act 2018, the Councils data retention policy and the Criminal Procedures Investigation Act |(CPIA).This will ensure that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworkswill ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.

9.2 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. This obligation applies equally to disclosure to additional persons within the Council and to disclosure outside the authority.

Storage

9.3 Material obtained through covert surveillance or property interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise risk. It must be held so as to be inaccessible to persons who would not need to see it (where applicable). This requirement applies to all those who are responsible for the handling of the material.

9.4 Any breaches of data protection requirements should be reported to the Councils DPA Officer and the SRO as it is likely to constitute an error

10 Errors

10.1 Proper application of the surveillance provisions in the RIPA codes should reduce the scope for making errors.

10.2 An error must be reported if it is a “relevant error”. A relevant error for is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act (RIPA).

10.3 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

10.4 Errors can have very significant consequences on an affected individual’s rights. All relevant errors made by public authorities must

Formatted: Font: Bold
Formatted: Default Paragraph Font, Font: Not Bold
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Bold, Not Italic, Font color: Red
Formatted: Justified
Formatted: Font: Bold
Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Justified
Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Justified
Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Justified
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted: Justified, Indent: Left: 1.27 cm, No bullets or numbering
Formatted: Left, Indent: Left: 0.32 cm, Hanging: 0.95 cm, No bullets or numbering
Formatted: List Paragraph, Justified, Indent: Left: 2.54 cm
Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm

be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error as soon as reasonably practicable and a full report no later than ten working days. The report should include information on the cause of the error; the amount of surveillance or property interference conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

Serious Errors

10.5 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

10.6 It is important that all staff involved in the RIPA process report any issues so they can be assessed as to whether it constitutes an error which requires reporting.

~~9~~11 Complaints

~~9~~11.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers, including those covered by this code, and is the only appropriate tribunal for human rights claims against the intelligence services. Any complaints about the use of powers as described in this code should be directed to the IPT.

11.2 The IPT is entirely independent from Her Majesty's Government and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for these purposes includes an organisation, an association, or combination of persons (see section 81(1) of RIPA), as well as an individual.

~~*There is provision under RIPA for the establishment of an Independent Tribunal. This Tribunal is will be made up of senior members of the legal profession or judiciary and will be independent of the government.*~~

Formatted: Font: Bold
Formatted: Justified, Indent: First line: 1.27 cm
Formatted: Justified
Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Justified
Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Justified
Formatted: Default Paragraph Font, Font: Not Bold
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Bold
Formatted: Default Paragraph Font, Font: Not Bold
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font, Font: 11 pt
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font, Font: 11 pt
Formatted: Font: 11 pt, Not Italic, Font color: Red
Formatted: Left, Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt
Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Strikethrough

~~4.2 The Tribunal has full powers to investigate and decide upon complaints made to them within its jurisdiction, including complaints made by a person who is aggrieved by any conduct to which Part II of RIPA applies, where he believes such conduct to have taken place in "challengeable circumstances" or to have been carried out by or on behalf of any of the intelligence services.~~

~~4.3 Conduct takes place in "challengeable circumstances" if it takes place:~~

~~(i) with the authority or purported authority of an authorisation under Part II of the Act; or~~

~~(ii) the circumstances are such that it would not have been appropriate for the conduct to take place without authority; or at least without proper consideration having been given to whether such authority should be sought.~~

~~11.3.~~4 Further information on the exercise of the Tribunal's functions and details of the relevant complaints procedure can be obtained from:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Tel 020 7273 4514

www.ipt-uk.com.

11.

4.~~5~~ Notwithstanding the above, members of the public will still be able to avail themselves of the Council's internal complaints procedure, where appropriate, which ultimately comes to the attention of the Local Government Ombudsman.

~~5~~12 Oversight by Investigatory Powers Commissioner

~~The Office of Surveillance Commissioners~~

12.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers to which this code applies, and adherence to the practices and processes described in it. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to

Formatted: Strikethrough
Formatted: Default Paragraph Font
Formatted: Default Paragraph Font
Formatted: Left, Indent: Left: 0 cm, Hanging: 1.27 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Left, Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font
Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font, Font: Bold
Formatted: Indent: Left: 0 cm, Hanging: 0.95 cm
Formatted: Default Paragraph Font, Font: Bold
Formatted: Font: Bold, Not Italic, Font color: Red
Formatted: Default Paragraph Font
Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font, Font: 11 pt, Not Bold
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font, Font: 11 pt
Formatted: Font: 11 pt

assist the Commissioner in his or her work. The Commissioner will also be advised by the 'Technology Advisory Panel'.

12.2 One of the duties of the IPCO is to carry out planned inspections of those public authorities who carry out surveillance as specified in RIPA, to ensure compliance with the statutory authorisation procedures. At these inspections they have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. All relevant persons using investigatory powers must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner.

~~*5.1 The Act also provides for the independent oversight and review of the use of the powers contained within Part II of RIPA, by a duly appointed Chief Surveillance Commissioner.*~~

~~*5.2 The Office for Surveillance Commissioners (OSC) was established to oversee covert surveillance carried out by public authorities and within this Office an Inspectorate has been formed, to assist the Chief Surveillance Commissioner in the discharge if his review responsibilities.*~~

~~*5.3 One of the duties of the OSC IPCO is to carry out planned inspections of those public authorities who carry out surveillance as specified in RIPA, to ensure compliance with the statutory authorisation procedures. At these inspections they have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties*~~

~~*, policies and procedures in relation to directed surveillance and CHIS operations will be examined and there will be examined and there will be some random sampling of selected operations. The central record of authorisations will also be inspected. Chief Officers will be given at least two weeks' notice of any such inspection.*~~

~~5~~12.3~~.4~~ An inspection report will be presented to the Chief Officer, which should highlight any~~,~~ significant issues~~,~~ draw conclusions and make appropriate recommendations. The aim of inspections is to be helpful rather than to measure or assess operational performance.

~~5.~~12.4~~5.~~ In addition to routine inspections, spot checks may be carried out from time to time.

12.5~~5.6~~ There is a duty on every person who uses the powers provided by Part II of RIPA, which governs the use of covert surveillance or~~,~~ covert ~~,~~human intelligence sources, to disclose or provide to

Formatted: Font: 11 pt
Formatted: Justified
Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Font: 11 pt
Formatted: Strikethrough
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Left, Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Font color: Auto
Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Font: 11 pt, Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Font: 11 pt, Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Font: 11 pt, Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto
Formatted: Font: 11 pt, Font color: Auto
Formatted: Default Paragraph Font, Font: 11 pt, Font color: Auto

the Chief Commissioner (or his duly appointed Inspectors) all such documents and information that he may require for the purposes of enabling him to carry out his functions.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: 11 pt, Not Bold

Formatted: Indent: Left: 0 cm, First line: 0 cm

PART 2 DETAILED PROCEDURE FOR UNDERTAKING DIRECTED COVERT SURVEILLANCE

1. Purpose

1.1 To ensure that surveillance is only undertaken in appropriate cases, is properly authorised and recorded and is compliant with the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and appropriate Code of Practices, made there under.

2. Scope

2.1 This procedure must be complied with by all sections and Investigating Officers, who routinely or occasionally undertake covert directed surveillance in connection with preventing or detecting crime with a maximum 6 months imprisonment or relate to the sale of alcohol or tobacco to children (the only permitted purpose for such surveillance). Local investigation procedures should make reference to this policy.

3. Procedure

3.1 It is very important that the correct authorisation procedure is followed prior to undertaking surveillance activity. Interference of the right to privacy without proper authorisation may render any evidence obtained unusable in a criminal court. If surveillance is conducted on individuals without the necessary authorisation, the Council and possibly individuals may be sued for damages for a breach of Human Rights. In civil matters adverse inferences may be drawn from such interference.

3.2 This procedure is supported by the Home Office "Code of Practice – Covert Surveillance" which is available on the Home Office website. If the surveillance is not likely to obtain private information, the codes do not apply. All Investigating Officers and Authorising Officers should fully acquaint themselves with the Code of Practice and refer to it during both the application and authorisation processes. ~~I THINK THE CODES SHOULD BE ON YOUR INTRANET~~

Formatted: Font color: Accent 6

3.3 All directed covert surveillance activity must be approved prior to the activity taking place by an Authorising Officer and a Justice of the Peace ("JP"). Officers seeking authority to undertake surveillance should complete the form, "Application for use of Directed Covert Surveillance". A sample application form with notes is attached at **Appendix 1**, but the latest version from the Gov.UK website must always be used. Completed application forms should be forwarded to the relevant Authorising Officer.

3.4 Completed authorisation forms should be allocated a reference number by the Investigating Officer relevant to the department / team and the particular investigation. The Investigating Officer should also obtain the next unique reference number from the Central Record of RIPA Applications and Authorisations maintained by the Principal Legal Executive.

3.5 The Authorising Officer will consider the completed application form and inform the Investigating Officer of his / her decision. The Authorising Officer will retain a copy of the authorisation form and monitor this for review, renewal and cancellation should it be approved by a JP. The original will be required to be returned to the applicant if authorised to be presented before a JP. If refused by the Authorising Officer or JP the original will be forwarded to the Principal Legal Executive for filing.

3.6 In addition the Authorising Officer must notify the Chief Executive & Town Clerk of an authorisation. ~~IS THIS STILL NECESARY~~

Formatted: Font color: Accent 6

3.7 The Investigating Officer and the Authorising Officer must give consideration to the following factors:

- **Necessity** – is covert surveillance the only or best way to retrieve the desired information, or is other less invasive methods appropriate?

- **Proportionality:**

  - balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

  - explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

  - considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and

- evidencing, as far as reasonable practicable, what other methods had been considered and why they were not implemented.

- **Collateral intrusion** – that is the obtaining of information relating to persons other than the subject of the investigation and the need to minimise this.

- **Confidential Information -** The Investigating Officer and the Authorising Officer must consider the possibility that the surveillance activity may result in the acquiring of confidential information. If this is considered to be likely then the Investigating Officer must highlight this on the application.

3.8 All Investigating Officers completing RIPA applications must ensure that applications are sufficiently detailed. When completing an application or authorisation, the applicant and authorising officer must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation. Authorising Officers should refuse to authorise applications that are not to the required standard and should refer them back to the Investigating Officers.

3.~~9~~8 **Magistrates' Court Approval:** As from the 1st November 2012 all applications and renewals for Directed Covert Surveillance and use of a CHIS will be required to have a JP's approval.

3.~~10~~9 Having had the activity authorised by the Authorising Officer, the Investigating Officer must now complete the relevant Judicial Approval form to seek approval from a JP. The Investigating Officer must ensure compliance with the statutory provisions and should refer to the Home Office publication (October 2012) "Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance"

https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa).

3.~~11~~10 The Judicial Approval form (see **Appendix 2**) will be submitted to the JP for approval. The form requires the Investigating Officer to provide a brief summary of the circumstances of the case on the judicial application form.

3.~~12~~11 The contact numbers for Her Majesty's Court and Tribunals Service to arrange a hearing is:

Formatted: Indent: Left: 2.54 cm, No bullets or numbering

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

Formatted: Font color: Red

Formatted: Indent: Hanging: 1.27

- Within office hours 01245 313315 or 01245 313313
- If out of hours the contact numbers are 07736 638551 or 07774 238418 ~~ARE THESE NUMBERS STILL CORRECT~~

Formatted: Font color: Accent 6

3.1~~3~~2 At the hearing which is on oath, the officer must present to the JP:

Formatted: Font color: Red

- the partially completed judicial approval/ order form;
- a copy of the RIPA application / authorisation form, together with any supporting documents setting out the case, and
- the original application / authorisation form (this must be retained by Investigating Officer).
- *It is preferred that the Authorising Officer also attends the hearing at the Magistrates Court*

3.1~~4~~3 The JP will consider the paperwork and may ask questions to clarify points or require additional reassurance on particular matters.

The JP will:

- Consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate;
- Consider whether there continues to be reasonable grounds;
- Consider whether the person who granted the authorisation or gave the notice was an appropriate designated person within the Local Authority, and
- Consider whether if the authorisation was made in accordance with the law, i.e. that the crime threshold for directed covert surveillance has been met.

3.1~~5~~4 The JP may:

- Decide to approve the Grant or renewal of an authorisation which will then take effect and the Local Authority may proceed to use the technique in that particular case, or
- Refuse to approve the grant or renewal of an authorisation in which case the RIPA authorisation will not take effect and the Local Authority may not use the technique in that case.

3.1~~6~~5 Where an application has been refused the Investigating Officer should consider the reasons for that refusal. If more information was required

by the JP to determine whether the application / authorisation has met the tests, and this is the reason for refusal, the Investigating Officer should consider whether they can reapply, for example, if there was information to support the application which was available to the Local Authority, but not included in the papers provided at the hearing.

3.17~~6~~ Where the JP refuses to approve the application / authorisation or renew the application / authorisation and decides to quash the original authorisation or notice the court must not exercise its power to quash the application / authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform Legal Services who will consider whether to make any representations.

3.18~~7~~ Whatever the decision, the JP will record their decision on the order section of the judicial application / order form. The court will retain the copy of the Local Authority RIPA application and authorisation form and the judicial application / order form. The officer will retain the original application / authorisation and a copy of the judicial application / order form.

3.19~~8~~ As previously stated the Principal Legal Executive is responsible for giving each authorisation a central unique identification number using a standard consistent format and recording it in a Central Record of RIPA Applications and Authorisations. This is to ensure that an up-to-date central record is maintained for all directed covert surveillance activity. Similarly, copies of all cancellations, renewals and review applications should be forwarded to the Principal Legal Executive promptly. The original authorisation should be kept on the investigation file.

~~3.19 The Investigating Officer and the Authorising Officer must consider the possibility that the surveillance activity may result in the acquiring of confidential information. If this is considered to be likely then the Investigating Officer must highlight this on the application. MOVED TO EARLIER~~

3.20 Written surveillance authorisations last for a maximum of three months. They cannot be authorised for a lesser period and the commencement date is the date approved by the J.P.. —Surveillance authorisations must be cancelled when no longer required (see 3.30 below).

~~3.21 All Investigating Officers completing RIPA applications must ensure that applications are sufficiently detailed. Authorising Officers should refuse to authorise applications that are not to the required standard and should refer them back to the Investigating Officers.~~

~~3.22 **Review:** Any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in the further or greater intrusion into the private life of any person should be brought to the attention of the Authorising Officer by means of a review.~~

Formatted: Strikethrough

Formatted: Font color: Accent 6, Not Strikethrough

Formatted: Strikethrough

Formatted: Font color: Red

Formatted: Strikethrough

Reviews

3.2~~13~~ The Authorising Officer has the responsibility to set the review dates for each authorisation and will determine what the review dates will be. The review date is detailed on the authorisation form. The review date will be at most one month from the date approved by the JP or previous review. The Authorising Officer should conduct the review with the Investigating Officer. Reviews should not be conducted solely by the Investigating Officer. Details of the review should be recorded on the form "Review of the use of Directed Surveillance Authorisation", available on the Home Office website and retained with the original authorisation. The Authorising Officer must ensure through diarisation or otherwise that reviews are conducted at the correct date.

3.22 Any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in the further or greater intrusion into the private life of any person should be brought to the attention of the Authorising Officer by means of a review. MOVED FROM EARLIER

3.2~~34~~ There is no requirement for a review form to be submitted to a JP. However if a different surveillance techniques is required it is likely a new application will have to be completed and approved by a JP.

Renewal

3.2~~45~~ ~~**Renewal:**~~ Should it be necessary to renew a Directed Covert Surveillance or CHIS application / authorisation, this must be approved by a JP.

3.2~~56~~ Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application).

3.2~~67~~ The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

3.2~~78~~ Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

Formatted: Font: Bold, Font color: Red
Formatted: Font: Bold, Font color: Red
Formatted: Left, Indent: First line: 0 cm
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Font color: Accent 6
Formatted: Font: Bold
Formatted: Font: Bold
Formatted: Indent: First line: 0 cm

3.2~~89~~ If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the Authorisation Officer authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

Formatted: Indent: First line: 1.27 cm

3.2~~930~~ ~~Cancellation~~ The Investigating Officer must complete the "Cancellation of the use of Directed Covert Surveillance" form available on the Home Office website and forward to the Authorising Officer who granted or last renewed the authorisation. It must be cancelled if they are satisfied that the directed covert surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

3.3~~01~~ As soon as the decision is taken that directed covert surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the Investigating Officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the Central Record of RIPA Applications and Authorisations along with a note of the amount of time spent on the surveillance.

3.3~~12~~ The officer submitting the cancellation must complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer must then take this into account and issues instructions regarding the management and disposal of the images etc.

3.3~~23~~ The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer. This will assist with future audits and oversight.

4. Joint Agency Surveillance

4.1 In cases where one agency is acting on behalf of another, it is usually for the lead agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the

Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

4.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also inform the Senior Responsible Officer or the Principal Legal Executive of the unique reference number, the agencies involved and the name of the officer in charge of the surveillance.

Formatted: Left

PART 3 DETAILED PROCEDURE FOR USE OF COVERT HUMAN ~~INTE~~ INTELLIGENCE SOURCES (CHIS)

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Left, Indent: Left: 0 cm, First line: 0 cm

Formatted: Font: Not Bold

1. Purpose

1.1 To ensure that CHIS activity is only undertaken in appropriate cases is properly authorised and recorded and is compliant with the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 and the appropriate Code of Practices, made there under.

2. Scope

2.1 This procedure applies to all usage of under-cover officers or informants, referred to as Covert Human Intelligence Sources (CHIS). This procedure does not apply to members of the public or Council officers who volunteer information pertaining to other individuals unless they are required to form a relationship with those other individuals.

2.2. Test purchase activity does not in general require authorisation under RIPA as vendor-purchaser activity does not constitute a relationship. However, if a number of visits are undertaken a relationship may be established and authorisation as a CHIS should be considered. Equally a test purchase may meet the definition of directed surveillance.

Formatted: Font color: Red

2.3 All sections ~~of the Council who routinely or occasionally~~ *that* undertake CHIS activity must comply with this procedure and ensure that their local procedures make reference to this document.

Formatted: Font: 11 pt

Formatted: Font: 11 pt, Font color: Red

Formatted: Font: 11 pt

2.4 Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice.

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

3. Procedure

3.1 It is very important that the correct authorisation procedure is followed prior to undertaking CHIS activity. Interference of the right to privacy without proper authorisation may render any evidence obtained unusable in a criminal court. If CHIS activity is conducted without the necessary authorisation, the Council and possibly individuals may be sued for damages for a breach of Human Rights. In civil matters adverse inferences may be drawn from such unlawful interference.

3.2 This procedure is supported by the Home Office "The Use of Covert Human Intelligence Sources" Code of Practice, which is available on the Gov.UK website. All Investigating Officers and Authorising Officers should fully acquaint themselves with the Code of Practice and refer to

it during both the application and authorisation processes. I think these should be ion the intranet

3.3 All CHIS activity must be authorised ~~approved~~ and approved by a JP prior to the activity taking place. ~~by an Authorising Officer and a Justice of the Peace ("JP").~~ Officers seeking authority to undertake CHIS activity should complete the form "Application for the Use of a Covert Human Intelligence Source (CHIS)" available from the Home Office Website. Completed application forms should be forwarded to the relevant Authorising Officer.

3.4 Within the provisions there has to be:

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare **(Handler)**

(b) at all times there will be another person who will have general oversight of the use made of the source **(Controller)**

(c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

The **Handler** will have day to day responsibility for:

- dealing with the source on behalf of the Local Authority concerned ;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

The Controller will be responsible for the general oversight of the use of the source.

3.5 **Tasking** is the assignment given to the source by the Handler or Controller such as by asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant Local Authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

3.6 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task.

Formatted: Font color: Accent 6

Formatted: Font color: Red

Formatted: Strikethrough

Formatted: Font color: Red

Formatted: Strikethrough

Formatted: Font color: Red

Formatted: Font color: Red

3.7~~6~~ Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship.

3.8 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual. ~~a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.~~

Use of equipment by a CHIS

3.9 If a CHIS is required to wear or carrying a surveillance device such as a covert camera it does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.

3.10 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations

~~**3.87 Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice. MOVED TO EARLIER**~~

3.11 All officers completing CHIS applications and in particular officers authorising applications must ensure that applications are sufficiently detailed. Authorising Officers should refuse to authorise applications that are not to the required standard and should refer them back to the originating officers~~. MOVED TO HERE MORE APROPRIATE~~

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font: Not Italic, Font color: Red

Formatted: Font color: Red

Formatted: Strikethrough

Formatted: Font color: Red

Formatted: Indent: First line: 1.27 cm

Formatted: Font color: Red

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

Formatted: Strikethrough

Formatted: Font color: Accent 6, Not Strikethrough

Formatted: Strikethrough

Formatted: Font color: Red

Formatted: Font color: Accent 6

3.12 The Investigating Officer and the Authorising Officer must consider the possibility that the CHIS activity may result in the acquiring of confidential information. If this is considered to be likely then the investigating officer must state this on the application. MOVED TO HERE

~~33~~.13~~8~~ Application forms should be allocated a reference number by the applicant relevant to the department and the particular investigation. The reference number should also reflect the number of authorisations in respect of the investigation.

3.14~~3.9~~ The application for authorisation must include full details of the reason for the CHIS and the intended outcome of the activity. The necessity for the CHIS activity should be explained. The CHIS activity must be proportionate to the potential offence or irregularity under consideration and should only be used when other methods of less intrusive investigation have been attempted or are not appropriate. CHIS authorisation forms must include enough detail for the Authorising Officer to make an assessment of the necessity and proportionality of the application. The application form must include details of the resources to be applied, the anticipated start date and duration of the activity, if necessary broken down over stages. Details should also be given of any CHIS activity previously conducted on the individual.

3.15~~0~~ The authorisation request should be accompanied by a risk assessment, giving details of how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with responsibility for maintaining a record of the use made of CHIS. The risk assessment should take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset. ~~Completed authorisation forms should be allocated a reference number by the Investigating Officer relevant to the department / team and the particular investigation. The Investigating Officer should also obtain the next unique reference number from the Central Record of RIPA Applications and Authorisations maintained by the Principal Legal Executive.~~ ~~REPEATED FROM ABOVE~~

3.16~~1~~ The Authorising Officer will consider the completed application form and inform the officer making the application of his decision. The Authorising Officer will retain a copy of the authorisation form and monitor this for review, renewal and cancellation.

3.17 ~~—~~In addition the Authorising Officer must notify the Chief Executive & Town Clerk of an authorisation

Formatted: Font color: Red

Formatted: Font color: Accent 6

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

Formatted: Strikethrough

Formatted: Font color: Accent 6

3.182 The Investigating Officer requesting authorisation for CHIS activity must give consideration to the following factors:

- **Necessity** – is the use of the CHIS covert activity ~~is covert surveillance~~ the only or best way to retrieve the desired information or is other less invasive methods appropriate.

Formatted: Font color: Auto

Formatted: Strikethrough

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm

Formatted: Font color: Red

Formatted: Font color: Auto

Formatted: Indent: Left: 2.54 cm, No bullets or numbering

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Formatted: Indent: Left: 0.63 cm, First line: 0 cm

Formatted: Font color: Auto

Formatted: List Paragraph, Indent: First line: 0 cm, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm

- **Proportionality** – is the CHIS covert activity ~~surveillance activity~~ proportional to the evidence that will be obtained and how it will benefit the investigation against the ~~and~~ intrusion into ~~to~~ the privacy of the subject and others that may be affected, ~~could reasonably expect or the~~. Are the methods used excessive and are they as non-invasive as is possible, and does the activity ~~surveillance~~ restrict an individual's right for privacy more than is absolutely necessary. ~~To demonstrate proportionality it is useful to compare the cost of the proposed surveillance activity with the scope of the problem and the potential impact on those impacted by the problem, and to identify how much the activity will impinge on the subjects. I DON'T THINK THIS IS APPROPRIATE DUSCUSS~~

3.19 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought.

3.20 Collateral intrusion – is the obtaining of information relating to persons other than the subject of the investigation. The application must show what steps are to be taken so as to minimise collateral intrusion.

3.21~~13~~ **Magistrates Court Approval:** As stated above from the 1st November 2012 all applications and renewals for Directed Covert Surveillance and use of a CHIS will be required to have a JP's approval. The procedure of obtaining the JP approval is the same as directed surveillance mentioned earlier.

Formatted: Font color: Red
Formatted: Font color: Auto, Strikethrough
Formatted: Font color: Auto
Formatted: Font color: Red
Formatted: Font color: Auto
Formatted: Strikethrough
Formatted: Font color: Auto
Formatted: Strikethrough
Formatted: Font color: Auto
Formatted: Font color: Red
Formatted: Font color: Auto
Formatted: Font color: Red
Formatted: Font color: Auto
Formatted: Strikethrough
Formatted: Font color: Auto
Formatted: Font color: Auto, Strikethrough
Formatted: Font color: Auto
Formatted: Strikethrough
Formatted: Font color: Auto
Formatted: Font color: Accent 6, Not Strikethrough
Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Font color: Red
Formatted: Indent: Left: 0.95 cm, First line: 0 cm
Formatted: List Paragraph, Left, Bulleted + Level: 3 + Aligned at: 3.17 cm + Indent at: 3.81 cm
Formatted: Font color: Red
Formatted: Left
Formatted: List Paragraph, Left, Bulleted + Level: 3 + Aligned at: 3.17 cm + Indent at: 3.81 cm
Formatted: Font color: Red
Formatted: Left
Formatted: List Paragraph, Left, Bulleted + Level: 3 + Aligned at: 3.17 cm + Indent at: 3.81 cm
Formatted: Font color: Red
Formatted: Left
Formatted ...
Formatted ...
Formatted: Font color: Red
Formatted ...
Formatted: Left
Formatted: Font color: Red

3.14 ~~Having received approval from an Authorising Officer the Investigating Officer must now complete the relevant application form to seek approval from a JP. An application form is attached at **Appendix 2**. The Investigating Officer must ensure compliance with the statutory provisions and should see the Home Office publication (October 2012) "Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) Home Office guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance"~~

~~https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa~~

~~3.15 The application form will be submitted to an Authorising Officer for consideration. The form requires the Investigating Officer to provide a brief summary of the circumstances of the case on the judicial application form.~~

3.16 ~~The contact numbers for Her Majesty's Court and Tribunals Service to arrange a hearing is:~~

- ~~Within office hours 01245 313315 or 01245 313313~~
- ~~If out of hours the contact numbers are 07736 638551 or 07774 238418~~

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Indent: Left: 0 cm, Hanging: 0.95 cm

3.17 ~~At the hearing, the officer must present to the JP:~~

- ~~the partially completed judicial application/order form;~~
- ~~a copy of the RIPA application / authorisation form, together with any supporting documents setting out the case, and~~
- ~~the original application / authorisation form (this must be retained by Investigating Officer).~~

~~3.18 The JP will consider the paperwork and may ask questions to clarify points or require additional reassurance on particular matters.~~

~~The JP will:~~

- ~~Consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate;~~
- ~~Consider whether there continues to be reasonable grounds;~~
- ~~Consider whether the person who granted the authorisation or gave the notice was an appropriate designated person within the Local Authority, and~~
- ~~Consider whether the authorisation was made in accordance with the law.~~

~~3.19 The JP may:~~

- ~~Decide to approve the Grant or renewal of an authorisation which will then take effect and the authority may proceed to use the technique in that particular case; or~~
- ~~Refuse to approve the grant or renewal of an authorisation in which case the RIPA authorisation will not take effect and the Local Authority may not use the technique in that case.~~

~~3.20 Where an application has been refused the Investigating Officer should consider the reasons for that refusal. If more information was required by the JP to determine whether the application / authorisation has met the tests, and this is the reason for refusal the Investigating Officer should consider whether they can reapply, for example, if there was information to support the application which was available to the Local Authority, but not included in the papers provided at the hearing.~~

Formatted: Strikethrough

Formatted: Strikethrough

~~3.21 Where the JP refuses to approve the application / authorisation or renew the application / authorisation and decides to quash the original authorisation or notice the court must not exercise its power to quash the application / authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform Legal Services who will consider whether the Council should make any representations.~~

~~3.22 Whatever the decision, the JP will record their decision on the order section of the judicial application / order form. The court will retain the copy of the Local Authority RIPA application and authorisation form and the judicial application / order form. The officer will retain the original application / authorisation and a copy of the judicial application / order form.~~

~~The original application and the copy of the judicial application / order form must be forwarded to the Principal Legal Executive for the Central Record of RIPA Applications and Authorisations.~~

3.~~23~~22 The original application and the copy of the judicial application / order form must be forwarded to the Principal Legal Executive promptly before the CHIS activity commences to ensure it meets all the necessary requirements. As previously stated Principal Legal Executive is responsible for giving each authorisation a central unique identification number using a standard consistent format and recording it in a central register. This is to ensure that an up-to-date central record is maintained for all CHIS activity. Similarly, copies of all cancellations, renewals and review applications should be forwarded to the Principal Legal Executive promptly. The original authorisation should be kept on the investigation file.

3.24 ~~All Investigating Officers completing CHIS applications must ensure that applications are sufficiently detailed. Authorising Officers should refuse to authorise applications that are not to the required standard and should refer them back to the Investigating Officers.~~ ~~REPEATED~~

3.25 ~~All officers completing CHIS applications and in particular officers authorising applications must ensure that applications are sufficiently detailed. Authorising Officers should refuse to authorise applications that are not to the required standard and should refer them back to the originating officers.~~ ~~MOVED TO EARLIER~~

3.26 ~~The Investigating Officer and the Authorising Officer must consider the possibility that the CHIS activity may result in the acquiring of confidential information. If this is considered to be likely then the investigating officer must state this on the application.~~ ~~MOVED TO EARLIER~~

Formatted: Strikethrough

Formatted: Font color: Accent 6

Formatted: Strikethrough

Formatted: Font color: Accent 6

Formatted: Strikethrough

Formatted: Strikethrough

3.237 Written CHIS authorisations last for a maximum of 12 months and cannot be authorised for a lesser period.. CHIS authorisations should be cancelled when no longer required. The investigating officer should complete the "Cancellation of an Authorisation of the Use or Conduct of a Covert Human Intelligence Source (CHIS)" form available on the Home Offices website and forward to the relevant Authorising Officer.

Management

3.248 The operation will require managing by the handler and controller which will included ensuring that the activities of the source and the operation remained focused and there is no status drift, It is important that the intrusion is assessed to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The Authorising Officer should maintain general oversight of these functions.

~~Each CHIS should be managed through a system of tasking and review. Tasking is the assignment given to the CHIS by the Handler. The task could be asking the CHIS to obtain information, to provide access to information or to otherwise act for the benefit of the Council. The handler is responsible for dealing with the CHIS on a day to day basis, recording the information provided and monitoring the CHIS's security and welfare. The Authorising Officer should maintain general oversight of these functions. THIS WAS ALL REPEATED>~~

3.259 During CHIS activity there may be occasions when unforeseen action or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review ~~updated~~ and re-authorised (for minor amendments only) or it should be ~~cancelled~~cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the Authorising Officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

Review

3.2630 The authorising officer will stipulate the frequency of formal reviews and the controller should maintain an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation. This will not prevent additional reviews being conducted by the authorising officer in response to changing circumstances such as where the nature or extent of intrusion into the private or family life of any person becomes greater than that anticipated in the original authorisation, the authorising officer

Formatted: Font color: Red

Formatted: Font: Bold, Font color: Red

Formatted: Indent: First line: 0 cm

Formatted: Font color: Red

Formatted: Strikethrough

Formatted: Font color: Accent 6, Not Strikethrough

Formatted: Strikethrough

Formatted: Indent: First line: 0 cm

Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm

should immediately review the authorisation and reconsider the proportionality of the operation as mentioned earlier.

~~**3.30 Review:** Any proposed or unforeseen changes to the nature or extent of the surveillance operation which may result in the further or greater intrusion into the private life of any person should be brought to the attention of the Authorising Officer by means of a review.~~

3.27~~31~~ Each application should be reviewed after an appropriate period of time and at most one month after the authorisation or previous review. The responsibility for review rests with the Authorising Officer who should conduct the review with the Investigating Officer. Reviews should not be conducted solely by the Investigating Officer. ~~In some cases, the Authorising Officer may delegate the responsibility for conducting of reviews to a subordinate Officer.~~ The review should include a reassessment of the risk assessment, with particular attention given to the safety and welfare of the CHIS. The Authorising Officer should decide whether it is appropriate for the authorisation to continue. Details of the review should be recorded on the form "Review of a Covert Human Intelligence Source (CHIS) Authorisation" available on the Home Office website, and retained with the original authorisation. ~~Cases should be reviewed at no more than one month intervals.~~ ~~The Authorising Officer must ensure, through diarisation or otherwise, that regular reviews are conducted within the correct timeframe.~~ ~~REPEATED BELOW~~

3.28~~32~~ Details of the review should be recorded on the form "Review of the use of Directed Surveillance Authorisation", available on the Gov.UK website and retained with the original authorisation. The Authorising Officer must ensure through diarisation or otherwise that regular reviews are conducted within the correct timeframe.

3.29~~33~~ There is no requirement for a review form to be submitted to a JP. ~~However~~However, if a different surveillance techniques is required it is likely a new application will have to be completed and approved by a JP.

Renewal

3.30~~4~~ ~~**Renewal:**~~ Should it be necessary to renew a Directed Surveillance or CHIS application / authorisation, this must be approved by a JP.

3.31~~5~~ Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a Justice of the Peace to consider the application).

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Font color: Accent 6, Not Strikethrough

Formatted: Strikethrough

Formatted: Indent: First line: 0 cm

3.326 The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

3.337 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

3.348 If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the Authorisation Officer authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

3.359 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

Formatted: Indent: First line: 0 cm

3.3640 ~~**Cancellation**~~ The Investigating Officer must complete the "Cancellation of an authorisation for the use or conduct of a Covert Human Intelligence Source" form available on the Gov.UK website and forward to the Authorising Officer who granted or last renewed the authorisation. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

3.3741 As soon as the decision is taken that CHIS activity should be discontinued, the applicant or other Investigating Officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the Investigating Officer to cease such activity, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the Central Record of RIPA Applications and Authorisations.

3.3842 The officer submitting the cancellation should complete in detail the relevant sections of the form.

3.3943 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and

the Senior Responsible Officer. This will assist with future audits and oversight.

3.40 An assessment of the welfare and safety of the source should also be assessed, and any issues identified.

Record Management for CHIS

3.4114 **~~Record Management for CHIS~~** Proper records must be kept of the authorisation and use of a source. The particulars to be contained within the records are:

- the identity of the source;
- the identity, where known, used by the source;
- any relevant investigating authority other than the Local Authority maintaining the records;
- the means by which the source is referred to within each relevant investigating authority;
- any other significant information connected with the security and welfare of the source;
- any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
- the date when, and the circumstances in which the source was recruited;
- the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
- the periods during which those persons have discharged those responsibilities;
- the tasks given to the source and the demands made of him in relation to his activities as a source;
- all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm
Formatted: Font color: Red
Formatted: Font color: Red
Formatted: Indent: Left: 0.95 cm, First line: 0.32 cm, No bullets or numbering
Formatted: Font color: Red
Formatted: Font color: Auto
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted: Font color: Auto
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted: Font color: Auto
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted: Indent: Left: 1.25 cm, First line: 0 cm
Formatted: Font color: Auto
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted: Indent: Left: 1.25 cm, First line: 0 cm
Formatted: Font color: Auto
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted: Indent: Left: 1.25 cm, First line: 0 cm
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...

- the information obtained by each relevant investigating authority by the conduct or use of the source;
- any dissemination by that authority of information obtained in that way; and
- in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Further documentation

3.42 Records or copies of the following, as appropriate, will also be kept by the relevant authority for at least five years:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation; and
- the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.

Formatted: Indent: Left: 1.25 cm, First line: 0 cm
Formatted: Font color: Auto
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted: Indent: Left: 1.25 cm, First line: 0 cm
Formatted: Font color: Auto
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.9 cm + Indent at: 2.54 cm
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted ...
Formatted: Font color: Auto
Formatted ...
Formatted: Indent: Left: 1.59 cm

3.43 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS.

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm, No bullets or numbering

Formatted: Indent: Left: 0.95 cm, No bullets or numbering

Formatted: Indent: Left: 0 cm, Hanging: 0.95 cm, No bullets or numbering

RIPA FLOW CHART 1 : DIRECTED SURVEILLANCE

Requesting Officer (The Applicant) must:

. Read the Corporate Policy & Procedures Document and be aware of any other guidance

. Determine that directed surveillance is required (For CHIS see Flowchart 2).

. Assess whether authorisation will be in accordance with the law.

. Assess whether authorisation is necessary under RIPA and whether it could be done overtly.

. Consider whether surveillance will be proportionate.

. If authorisation is approved review or renew regularly with Authorised Officer.

If a less intrusive option is available and practicable : USE THAT OPTION! use that option.

If authorisation is necessary and proportionate, prepare and submit your application form to the Authorised Officer .

Authorised Officer must:

- Consider in detail whether all options have been duly considered, including the Corporate Policy & Procedures Document and any other guidance issued by the SRO
- Consider whether surveillance is considered by him/her to be in accordance with the law, necessary and proportionate.
- Authorise only if an overt or less intrusive option is not practicable.

The Applicant must:
REVIEW REGULARLY
And complete the review form and submit to Authorised

Authorised Officer must: If surveillance is still necessary and proportionate after authorised period:

- Renew authorisation
- Set an appropriate further review date and use

The Applicant must:
If operation is no longer necessary or proportionate, complete **CANCELLATION FORM** and submit to Authorised Officer

Authorised Officer must:
Cancel authorisation when it is no longer necessary or proportionate to need the same.

Essential
Applications for Directed Surveillance will be completed on the electronic database and need to be maintained appropriately. The electronic database forms the Central Database for RIPA.

NB if in doubt, ask the Group Manager (Legal and Democratic) BEFORE any directed surveillance and/or CHIS is authorised, reviewed, renewed, cancelled, or rejected.

Appendix 1 *(b)*

SAMPLE APPLICATION FORM FOR USE OF DIRECTED COVERT SURVEILLANCE

Unique Reference Number	Refer to your policy as to how you obtain the unique number. All applications must have one and put on each page.

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority *(including full address)*	State your Public Authority Name and full address

Name of Applicant	Details of the person completing the form	**Unit / Branch / Division**	Section and department
Full Address	Provide the address of your department		
Contact Details	Provide full contact details including email address. Make it easy for the Authorising Officer, or anyone else associated with the process to contact you.		
Investigation / Operation Name (if applicable)	This may be an investigation reference number allocated to this case, or some other reference		

Investigating Officer (if a person other than the applicant)	If the form is being completed by someone who is not the investigator, then the investigators details must be put in this box.

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]

s above.

or local authorities: The exact position of the authorising officer should be given. For xample, Head of Trading Standards.

lso use the description of the person's position contained within your policy to remove any onfusion.

Describe the purpose of the specific operation or investigation.

scribe the investigation to date including the offences and the relevant legislation. When, ere and how are the offences occurring. Remember the Authorising Officer needs to be ar what the offence is and the circumstances. (keep information relevant and to the point)

lude the details of the suspects and persons involved and the role they play within the estigation. (Do not put confidential information in such as informants' names)

nsider disclosure implications under CPIA with regards to not revealing unnecessary ormation. However, the AO needs sufficient relevant information to make a decision. The ovisions of using CPIA sensitive information may be a way of dealing with the sensitivity ues later, by editing material if it has to be disclosed. However, if the document contains nsitive information remember to keep it secure at all times.

oss reference where necessary to other relevant applications

Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

s should be completed, after attending the area of where the activity is to be carried out, d having carried out a surveillance assessment having taken into account risks or limiting tors. Limiting factors are anything can affect the success of the operation.

nsider the AO statement in box 12, the 5 WH. The applicant can only do what is authorised the AO, not what they have applied for.

nsider the aims and objectives, confirmation of address may only need static servations; however, lifestyle intelligence may require foot/mobile and use of covert meras etc.

at exactly do you want to do? Is it static observations, foot or mobile? You want a mbination? However, only ask for what you can realistically carry out. It is not a wish list; hould be carried out to achieve the objectives.

w do you want to carry out the surveillance and what equipment do you want to use? You st make the AO aware of the capabilities of any equipment you want to use.

ere is the activity to take place? Who is the activity against and when do you want to carry ut?

at is the expected duration? It does not mean that it must only be authorised to this point. ce signed, the authorisation lasts for a 3 month period. You must update the AO when y set the review dates. If your operation ends prior to any review date or the 3 month riod, you must cancel it straight away and submit the cancellation form. It does not expire.

MEMBER YOU CAN ONLY DO WHAT IS AUTHORISED ON THE AO SECTION, NOT WHAT U HAVE APPLIED FOR IN THIS SECTION.

The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

If you do not know who the subjects are, insert any descriptions you may have. If as a result of the surveillance, you identify anyone, you must submit this information on a review form to the AO.

Consider any known associates. If the intelligence is that the subject of the surveillance has known associates, are they likely to become subjects of the surveillance? If so, detail them as part of the application.

Explain the information that it is desired to obtain as a result of the directed surveillance.

ese are the surveillance objectives. They should have been identified during the planning ge and a feasibility study carried out to assess whether they can be achieved. It's no use ting objectives that can't be achieved.

at is the surveillance going to tell you?

at, if any, criminality will it establish?

l it identify subjects involved in criminality?

l it house subject or their criminal associates?

.

Identify the location of the subject's place of work

To gather intelligence and evidence to establish the extent of the criminality (size).

Identify other persons involved, such as suppliers.

Identify other premises involved, such as storage buildings.

Obtain best evidence through the use of photographic equipment to assist with ntifying the offenders

tain best evidence to assist with a prosecution of offenders

Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*

In the interests of national security;

For the purpose of preventing or detecting crime or of preventing disorder;

In the interests of the economic well-being of the United Kingdom;

In the interests of public safety;

For the purpose of protecting public health;

For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

r Directed Surveillance, Local Authorities only lawful purpose is preventing or detecting me and the crime must be capable of carrying six months imprisonment or criminal ences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.
e to the nature of the offences, if any other areas above are applicable such as protection public health, this should be made clear in the body of the application and the portionality section.

Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

u can reiterate the criminal offences

y is it necessary at this stage of the enquiry to carry out covert activity?

at is the purpose of the operation?

w will the activity assist or progress the investigation?

at will be the consequences of the proposed action be to the victim?

y do we need this evidence/intelligence/information?

nat other enquiries have been carried out and results? This does not have to be a last sort, but if there is a less intrusive way of achieving your objectives you should take that tion, or explain why you can't take that option.

nsequences of not taking action

s not for the applicant to state on the application that they believe it to be necessary. This the responsibility of the AO to reach that decision.

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

Describe precautions you will take to minimise collateral intrusion.

There are three parts to this section (see above). You must answer them all, as this section directly impacts upon the proportionality test.

1. SUPPLY DETAILS OF POTENTIAL COLLATERAL INTRUSION

Visit the location of where the activity is to take place and carry out a risk assessment. Who lives at the property that you may be watching. Have they got children who might be affected such as going to school etc.?

Determine where you need to be to carry out the surveillance. What else can you see?

What equipment will you be using and what will it see and record?

Consider Confidential Information

It may be useful to paint the picture in words of what it is you will be watching in the locality. This will assist the AO. You may also want to refer to any plans or maps attached to the application.

2. WHY IS THE INTRUSION UNAVOIDABLE?

Consider why the intrusion is unavoidable, such as the location and time frame that the observations have to be carried out. It may be that you are limited to the use of certain equipment only and therefore governed by its operating capabilities. Your observation position may be the only place you can use.

3. DESCRIBE THE PRECAUTIONS YOU WILL TAKE TO MINIMISE COLLATERAL INTRUSION

Having carried out the risk assessment and identified what the intrusion is, consider ways of reducing the intrusion, or keeping it to a minimum. You should consider:

State who the activity will be focused on, such as the subject etc., not the innocent third parties subject to the collateral intrusion.

Keeping the surveillance activity focussed with regards to length of time spent on the observations. However, remember that you still need time to achieve your objectives. You will need some flexibility built in to your timings.

If using technical equipment such as video or covert recordings, consider the position and focal length of the lenses when filming to reduce the intrusion. Consider when and who you will use the equipment against, such as the suspects only.

How will you manage any images obtained? Consider Data Protection, confidentiality, security, dissemination of the images, and any guidance provided by your organisation, including any Home Office guidance.

Are the staff trained to carry out the activity? If so, this may assist, as they should know what they are doing with regards to collateral intrusion.

The activity needs to be tightly managed and reviewed constantly. If there is a considerable change in the intrusion once the activity commences, then the AO needs to be made aware.

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

In the necessity box we stated why it was necessary to carry out the covert activity. In this box we are assessing whether the actions requested are proportionate to the overall operational aims within the investigation, having taken into account of the intrusion issues.

How serious are the offences under investigation? What is the direct or accumulative consequence of the offences?

What are the effects of the offences on the victim or the consequences of what is happening?

Are you asking to do a lot to achieve a little? Do not use a sledgehammer to crack the nut.

If you have provided a good explanation of how the intrusion will be reduced and managed in the collateral intrusion box, refer them to it.

Explain why you need to undertake this activity to achieve your objectives, against using other methods. Why, in operational terms, does your need to use the activity (how the activity will progress the investigation) outweigh the level of intrusion? Why is this method the least intrusive option?

Are your methods/tactics balanced in relation to the likely results?

Consider the length of time of the surveillance operation

What methods are required to achieve the objectives and are there any less intrusive methods? You should explain what if any less intrusive methods have been considered. If they can be used they should be. If however less intrusive methods cannot be used, explain why. You should also take account that technical surveillance may be more intrusive.

Consequences of not taking action.

10. Confidential information [Code paragraphs 4.1 to 4.31].

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Is there any likelihood of Health, Solicitors, Counselling, and Spiritual etc.

It is unlikely that you will obtain this type of material, but an assessment should take place. If you are, it is a higher level of Authorising Officer who needs to consider it.

Do not mix this up with Private Information which is part of the consideration when assessing whether the activity falls under RIPA.

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

REMEMBER THAT EACH CASE HAS TO BE ASSESSED ON ITS OWN MERITS.

Who are you authorising to carry out the activity? Are the staff from one office? Or if a joint operation, please state that fact and name the other organisation. You have to actually authorise the other organisation's staff in writing.

What are you authorising them to do and what equipment are you authorising them to use? You should have a knowledge of the equipments capability.

Who are you authorising them to do it against, person, address, vehicle,etc?

When are you authorising them to do it?

Where are you authorising the activity to take place?

Why are you authorising whatever you are allowing them to do? They should have stated within the application earlier what they are hoping to achieve.

When authorising the activity, it is live for 3 months. In other words, as an AO, you cannot authorise for less. You should set a review date for you to review it if you think that the surveillance should be a shorter period.

DO NOT BE AFRAID AS AN AO, TO ONLY ALLOW THEM TO UNDERTAKE CERTAIN ACTIVITY, AS OPPOSED TO ALL THE ACTIVITY APPLIED FOR, IF IT MEANS THAT IT IS PROPORTIONATE. STATE WHY ON THE FORM

IF NOT AUTHORISING, STATE WHY.

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3].

Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

IF YOU ARE WRITING IN THIS SECTION, PRINT THE FORM OUT WITH ENOUGH SPACE TO WRITE IN. YOU WILL REQUIRE SOME SPACE TO DETAIL HOW YOU HAVE COME TO YOUR DECISION.

Below are 5 areas that should be dealt with by the AO when considering the application.

Code 3.3 requires that the person granting an authorisation BELIEVES that the authorisation is necessary in the circumstances of the particular case for one of the statutory reasons (see box 6). Have they made clear what the offence or offences are in the body of the application?

Code 3.4 then if the activities are necessary, the person granting the authorisation must

BELIEVE that they are proportionate to what is sought to be achieved by carrying them out. AO must also BELIEVE that the objectives can't be met by other less intrusive means.

Sec 72 RIPA 2000, a person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71 shall, in doing so, HAVE REGARD TO THE PROVISIONS (so far as they are applicable) of every code of practice for the time being in force under that section. (You have to know what the codes say).

Collateral Intrusion Code of Practice 3.8 before authorising surveillance the authorising officer should also TAKE INTO ACCOUNT the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.

Code of Practice 3.15 .Any person granting or applying for an authorisation will also NEED TO BE AWARE OF particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

This will take some consideration. Read and study the application fully. Refer to the applicants boxes that deal with these issues.

Detail your thought processes. How have you come to the conclusion? Do not rubber stamp, do not use template or cut and paste answers. This is your original note that you may be relying on in court. If you are making decisions from reading supporting material, mention the material and keep a copy which needs to be part of the central register. Be careful to make your decisions on written material not discussions with the case officer which may be difficult to justify at a later date at court.

Model answer from codes and OSC

- **balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;**
- **explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;**
- **considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;**
- **evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.**

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.
This is completed by the AO who has the responsibility to consider the authorisation if confidential information is likely to be obtained. (Usually someone of a much higher position than a normal AO.) e.g. In a Local Authority it will be the Chief Executive. **See rear of codes of practice for relevant position and refer to your policy.**

Date of first review	**AO must set the review date. Consider what the applicant has stated regarding the length of time required. Remember, this is so you as the AO can now review the need for the activity to continue on the date you have set. Also refer to policy. Most state that it must not be longer than a month. However, you must assess it against all the facts.**

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

As above.

Name (Print)		Grade / Rank		
Signature		Date and time		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]			From 1 Nov 12 this date will be from when a Magistrate approves it. Put in the expiry date. Remember it lasts for 3 months once signed (see opposite)	

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

OSC guidance states that there is no longer a requirement to complete the whole application form; contemporaneous notes should have been made by both applicant and AO. However, check what your policy says as some organisations still require at least this part to be completed with certain other sections. If your policy does not make it clear, seek advice.

FROM 1 NOVEMBER 2012 THERE WILL BE NO URGENT PROVISIONA AVAILABLE FOR LOCAL AUTHORITIES

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

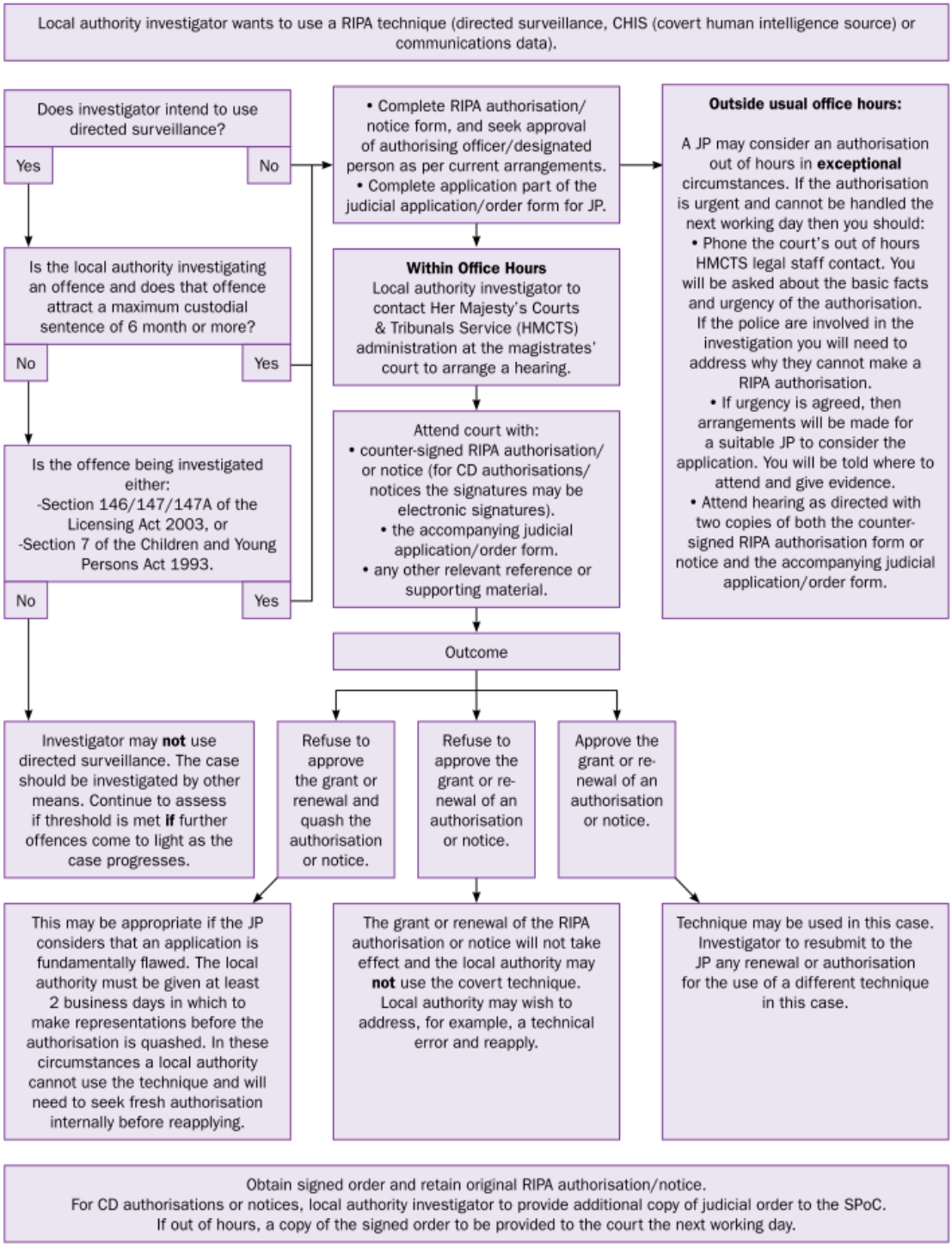
This is because the legislation allows for a lower rank/grade to authorise in urgent cases for some organisations. Refer to your policy.

See Statutory Instrument 2010 No 521.

Name (Print)		Grade/ Rank		
Signature		Date and Time		

Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Appendix 2 *(b)*

COPY APPLICATION FORM AND ORDER FOR JUDICIAL APPROVAL

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval
communications data, to use a covert human inte
surveillance. Regulation of Investigatory Powers A

Magistrates' court:.....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for belie
and remain satisfied, and that the relevant conditions a
renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisa

☐ refuse to approve the grant or renewal and quash the a

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court: